

ATTACHMENT C

AFFIDAVIT OF JOHN CHEVALIER

I, John Chevalier, Task Force Officer of the Federal Bureau of Investigation, Nashville Division, Memphis Resident Agency, being duly sworn, state that the following information is true and correct to the best of my knowledge, information and belief:

1. I am a Memphis Police Department Task Force Officer (TFO) assigned to the Federal Bureau of Investigation (FBI), Memphis Resident Agency. I have been employed by the Memphis Police Department since August 10, 1998. I have also been sworn as a Special Deputy United States Marshal. I am currently assigned full-time to the FBI's Memphis Child Exploitation Task Force. Throughout my law enforcement career, I have arrested countless individuals for violations of law. I have also participated in multiple search warrants leading to the seizure of items having evidentiary value; these seizures have aided in the successful arrest and prosecution of individuals involved in criminal activity. Since joining the Task Force I have received training on the investigation and prosecution of child exploitation cases and I have experience in Sex Crimes investigations, including working cold case sexual assault cases as a Memphis Police Officer. I was assigned to or participated in approximately 500 cold case investigations. I have gained experience through training in seminars, classes and everyday work related to conducting these types of investigations.

2. As a FBI Task Force Officer, your Affiant is authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq. Section 2251(a) makes it a federal offense for any person to employ, use, persuade, induce, entice, or coerce any minor (person under the age of 18) to engage in, or have a minor



assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or to attempt to do so. Section 2252(a) makes it a federal offense to knowingly possess, access, transport, receive, or distribute a visual depiction, the production of which involving the use of a minor engaging in sexually explicit conduct, if such visual depiction is of such conduct, or to attempt to do so, if that visual depiction has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, or the visual depiction was produced using materials that have been so mailed, shipped or transported. “Sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A), and includes sexual intercourse of any kind, whether between persons of the same or opposite sex; bestiality; masturbation; and the lascivious exhibition of the genital or pubic area.

3. Your Affiant has conducted and/or participated in investigations relating to the sexual exploitation of children. During these investigations I have observed and reviewed examples of child pornography in various forms of media including computer media. Your Affiant has received training and instruction in the field of investigation of child pornography, child sexual exploitation, and human trafficking, sexual enticement via social media applications and in the area of forensic extraction of digital evidence.

4. This application is part of an investigation into **Austin Pridmore** (hereinafter PRIDMORE) for the alleged online solicitation and enticement of minors.

5. The following information was obtained through observations and conversations of your Affiant personally, through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically named in this affidavit. Since this



affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violation of Title 18 U.S.C. §§ 2251 and 2252, and 2422, will be located on the device described in **Attachment A**, and consist of or be contained in the items listed in **Attachment B**, which are incorporated by reference as if fully set forth herein.

STATUORY AUTHORITY

6. Title 18 United States Code, Section 2251 provides in pertinent part that any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in; or who has a minor assist any other person to engage in; or who transports any minor in or affecting interstate or foreign commerce;...with the intent that the minor engage in...any sexually explicit conduct for the purpose of producing any visual depiction of such conduct...and the person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or be mailed; or if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, including by computer; or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or, in or affecting interstate or foreign commerce, or mailed, or attempts or conspires to do so, commits an offense against the United States.

7. Title 18, United States Code, Section 2252 provides in pertinent part that anyone who:

(a)(1) knowingly mails or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by



computer, any visual depiction if: A) producing the visual depiction involved the use of a minor engaging in sexually explicit conduct; and B) the visual depiction is of such conduct;

(a)(2) knowingly receives or distributes any visual depiction: using any means or facility of interstate or foreign commerce or the mail; or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce; or which contains materials that have been so mailed, shipped or transported if: A) producing the visual depiction involved the use of a minor engaging in sexually explicit conduct; and B) the visual depiction is of such conduct;

(a)(4)(B) knowingly possesses or accesses with intent to view any matter which contains any visual depiction that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or which was produced using materials that have been so shipped or transported if: A) producing the visual depiction involved the use of a minor engaging in sexually explicit conduct; and B) the visual depiction is of such conduct; or conspires or attempts to do so commits an offense against the United States.

“Sexually explicit conduct” is defined at 18 U.S.C. § 2256(A) as actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or the lascivious exhibition of the anus, genitals, or pubic area of any person.

8. Title 18, United States Code, Section 2422 provides in pertinent part that whoever knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, commits an offense against the United States.



PROBABLE CAUSE

9. On March 19, 2023 the Lauderdale County Tennessee Sheriff's Office received a telephone complaint regarding the rape of a 13-year-old female. Uniformed deputies were dispatched to investigate the complaint. Deputies met with Minor Victim and her mother. Minor Victim reported she met a male on Snapchat and that male raped her. A short time later, Minor Victim told a nurse at the Memphis Rape Crisis Center that the male picked her up at her home and drove her to a field, after which she asked to be let out of the truck. Instead, he took her clothes off, zip tied her hands together and "choked" her causing her to become unconscious. As she regained consciousness, the male was getting off her and putting his clothes on. She had pain in her vagina. The male dropped her off at a church where she got out of the truck and walked home. Your affiant is aware that it is common for people to use the term "choke" when referencing being strangled by having a hand or hands on one's neck restricting the ability to breath. The result of strangulation is often loss of consciousness.

10. The Minor Victim showed responding deputies the male's Snapchat account, justinp9131, on her cellular telephone. She believed his name to be Justin Parker. The account details listed Justin Parker to be single and 16 years old. She also showed deputies a picture of Justin Parker. Deputies recognized this person to be PRIDMORE. Minor Victim was shown a driver's license picture of PRIDMORE whom she identified him as the male that picked her up and raped her.

11. On that same day within hours of the rape being reported, Lauderdale County Deputies arrested PRIDMORE for the rape of Minor Victim. At the time of his arrest, PRIDMORE was in possession of a blue iPhone 13. The iPhone 13 was seized and turned over to the FBI.

12. On June 14, 2023 a federal search warrant was served upon Snapchat for justinp91321 and an additional Snapchat account of PRIDMORE's, justinstough22. Your affiant has reviewed these accounts. Chatting activity was active in the accounts up to PRIDMORE's March 19, 2023 arrest. PRIDMORE has been in law enforcement custody since then, currently housed in the Tennessee Department of Corrections.

13. During the review of Snapchat account justinp9131, three accounts have been identified sending PRIDMORE possible Child Sex Abuse Material (CSAM). IP data indicates an iPhone 9 and an iPhone 14 were used to access the Snapchat account in March 2023. On 3-19-2023 at 9:19 pm PRIDMORE blocked the Snapchat account of the Minor Victim's Snapchat account using an iPhone9.

14. On January 30, 2025 a federal search warrant was issued for the blue iPhone 13 seized from PRIDMORE at the time of his March 19, 2023 arrest. A review of this phone indicated the last activity to be in January 2022. The phone was using iCloud account austinpridmore454@icloud.com. The Device Summary Report generated during the forensic extraction of the iPhone 13 indicated the last iCloud backup date to be January 9, 2022, owner name Austin Pridmore, account austinpridmore454@icloud.com.

15. On March 4, 2025, Apple preserved all data associated with account austinpridmore454@icloud.com and provided case number 202500986237 for reference.

16. Your affiant is aware that an iCloud account can be shared with multiple devices. It is believed that evidence of PRIDMORE's criminal activity prior to and beyond January 2022 stored in iCloud account austinpridmore454@icloud.com will assist in this investigation. Your affiant is asking for the court's permission to search the aforementioned account.



BACKGROUND CONCERNING APPLE¹

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.
18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:
 - a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
 - b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
 - c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Manage and use your Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “Introduction to iCloud,” available at <https://support.apple.com/kb/PH26502>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; and “Apple Platform Security,” available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.



Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased

A handwritten signature in blue ink, appearing to read "JL".

through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.
20. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

A handwritten signature in blue ink, appearing to read "JL".

21. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

22. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.



23. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

24. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. As previously described, for instance, screenshots of messages between Graham and "Bae" about Young's cooperation to get his sentence reduced, which would be stored in iPhotos files in Graham's iCloud account, were sent to Young. Graham also has text messages, which could be in the iMessage files in Graham and Washington's iCloud accounts, discussing the criminal conduct, to include instructions about what Young needs to do in order to get his points reduced. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In this instance, evidence confirms that Graham sent screenshots of iMessage communications in furtherance of the facilitation of the bribery of a public official. The timestamps in the screenshotted messages coincide with timestamps from phone records of messages between Graham and Washington. Furthermore, phone records confirm frequent communication between Graham and Washington on SUBJECT ACCOUNTS 1 and 2 respectively.
26. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the

geographic and chronological context of access, use, and events relating to the crime under investigation.

27. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

28. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. Particularly, your Affiant believes communications concerning the facilitation of bribery of a public official, photographs of these communications, location data, contact information, and other evidence pertaining to the furtherance of this criminal activity will be present in the referenced iCloud accounts. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

29. On September 9, 2024, the Federal Bureau of Investigation served a preservation letter to Apple, Inc. for 90 days. The subsequent preservation extensions were served so the records would be preserved until May 25, 2025.

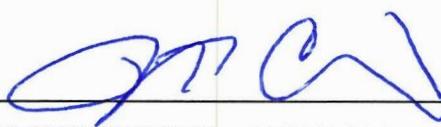
30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



CONCLUSION

31. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a search warrant for iCloud account austinpridmore454@icloud.com more specifically described in **Attachment A** which is incorporated herein, for the items described in **Attachment B**, incorporated herein.

AND FURTHER, AFFIANT SAITH NOT.



JOHN CHEVALIER - AFFIANT
Task Force Officer, Federal Bureau of Investigation

Sworn to before me in Memphis, Tennessee, this 2 day of April, 2025.



HON. TU M. PHAM UNITED STATES MAGISTRATE JUDGE